Je veux avoir le genre de pratiques de sécurité qui me permettent d'être ouverte tout en sachant que j'ai évalué les risques auxquels je suis exposée et que je prends des mesures intelligentes pour les minimiser. La culture de la sécurité devrait faciliter et non pas limiter l'ouverture aux autres. Cette proposition de culture de la sécurité repose sur un recadrage – sur le passage de la peur à l'assurance, de l'aversion au risque au courage, de l'isolement aux liens, et de la suspicion à la confiance.

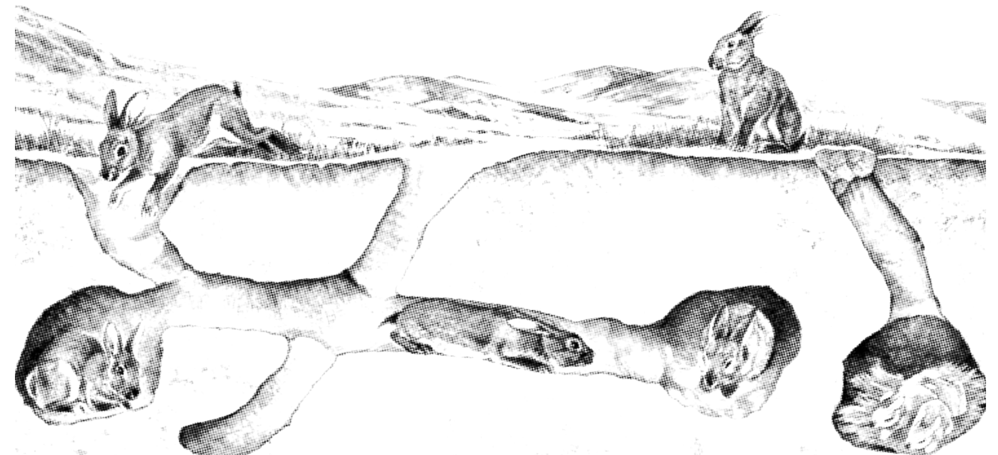


No Trace Project / Pas de trace, pas de procès. Un ensemble d'outils pour aider les anarchistes et autres rebelles à **comprendre** les capacités de leurs ennemis, **saper** les efforts de surveillance, et au final **agir** sans se faire attraper.

Selon votre contexte, la possession de certains documents peut être criminalisée ou attirer une attention indésirable—faites attention aux brochures que vous imprimez et à l'endroit où vous les conservez.

Assurance, courage, lien, confiance

Une proposition de culture de la sécurité



Assurance, courage, lien, confiance : Une proposition de culture de la sécurité

Texte d'origine en anglais

Confidence. Courage. Connection. Trust. A proposal for security culture

2019

north-shore.info/2019/11/05/confidence-courage-connection-trust-a-proposal-for-security-culture

Traduction et mise en page

No Trace Project

notrace.how/resources/fr/#assurance

police a fait une perquisition chez nous. Ils ont saisi une quinzaine d'ordinateurs portables et de téléphones ainsi que plusieurs clés USB et disques durs. Parmi tout ça, un seul ordinateur portable n'était pas chiffré car il était resté allumé. Mais sur tout le reste, aucune information n'a pu être récupérée. Les historiques des SMS et des appels qui été obtenus via nos opérateurs téléphoniques n'ont rien révélé puisqu'on utilise le chiffrement de bout en bout avec un service qui protège les métadonnées. On utilise pas les réseaux sociaux ou Google pour communiquer. Lorsqu'ils ont fait des recherches sur ces plateformes, ils n'ont rien trouvé. Ces pratiques de sécurité informatique fonctionnent lorsqu'elles sont appliquées correctement et de façon constante. Il y a une vraie différence entre les appliquer et ne pas les appliquer, en terme de résultat. Ces méthodes nous mettent en confiance lorsqu'on se lie aux autres et contribuent à construire la confiance.

Merci de votre lecture! Ce texte est plus long que prévu, mais j'espère qu'il a été utile. Je l'ai écrit car il n'y a pas une tonne de bonnes ressources à propos de culture de la sécurité. J'espère que ça inspirera les gens à discuter de quelles pratiques sont appropriées pour elleux, animés par un esprit d'assurance, de courage, de liens et de confiance. Par nos actes, gardons le cap sur le monde qu'on tente de créer plutôt que de craindre les mouvements de nos ennemi·e·s. Bonne chance !

plusieurs applications de messagerie la rendent très accessible. Je recommande Signal, de Open Whisper Systems, même si WhatsApp utilise le même type de protocole de chiffrement, mais sans protection des métadonnées. L'inconvénient est que ce ne sont pas des logiciels multiplateformes, alors qu'avec PGP, puisque c'est possible de copier-coller des blocs de textes, on peut l'utiliser avec tout—les différents clients de messagerie, Facebook, Twitter et même les messages textes. Mais c'est plus difficile de se mettre à PGP et l'expérience a démontré que les gens ne sont pas prêts à faire beaucoup d'efforts pour leur sécurité informatique.

Deux : Chiffre les données là où elles sont enregistrées. À moins d'avoir une raison de ne pas le faire, tu dois immédiatement chiffrer ton téléphone (Android a une option pour ça, de nombreux iPhones sont chiffrés par défaut). Pour les données enregistrées sur les ordinateurs, les disques durs externes, les clés USB ou en ligne, je recommande VeraCrypt. Ça te permet de faire des « boîtes » chiffrées où tu mets tes fichiers. Par contre, ça ne t'aidera pas si ton chiffrement est déverrouillé au moment où ton ordinateur est saisi. Si tu penses que tu risques d'être arrêté, ne circule pas entre différents endroits avec ton téléphone (chiffré) allumé. Envisage de récupérer un vieux réveille-matin. Ainsi, tu peux éteindre ton téléphone et ton ordinateur pendant la nuit (ce qui ré-active le chiffrement, typiquement désactivé au démarrage), particulièrement si tu risques d'être perquisitionné. Fais des sauvegardes de tes données et garde-les dans un autre lieu.

Trois : Dissimule ton identité en ligne lorsque c'est possible. Ton adresse IP est visible par tous les sites web et les services que tu utilises et relie tes activités du point de vue de ton fournisseur d'accès à Internet et de l'État, même si tu utilises la « navigation privée ». Je recommande l'utilisation de Tor pour toute navigation ou recherche. Les réseaux sociaux d'entreprises bloquent généralement Tor (Reddit est une exception et Twitter te laissera utiliser Tor si tu le leur demandes), donc si tu essaies d'avoir un compte anonyme sur ces réseaux, une option est d'utiliser un VPN—il y en a un gratuit et disponible chez Riseup[10] pour l'usage des anarchistes et des militants.

Beaucoup plus de choses peuvent être faites pour la sécurité informatique, mais ces trois étapes sont déjà un bon début. Il y a quelques années, la

[10]https://riseup.net

Quand on parle de culture de la sécurité, les gens vivent généralement l'une de ces deux expériences : soit iels construisent des murs et tiennent les autres à l'écart, soit iels sont iels-même exclu·e·s et n'ont pas la confiance des gens. Dans les deux cas, il y a des sentiments négatifs—la peur et la suspicion pour le premier et un sentiment d'aliénation et du ressentiment pour le second. Je dirais que ce sont les deux côtés d'une même médaille, deux expériences d'une culture de la sécurité qui ne fonctionne pas bien.

Je veux être accueillante et ouverte aux nouvelles personnes quand je m'organise. Je veux aussi me protéger du mieux possible des efforts visant à perturber cette organisation, surtout de la part de l'État, mais aussi des patrons ou de l'extrême-droite. Ça signifie que je veux avoir le genre de pratiques de sécurité qui me permettent d'être ouverte tout en sachant que j'ai évalué les risques auxquels je suis exposée et que je prends des mesures intelligentes pour les minimiser. La culture de la sécurité devrait faciliter et non pas limiter l'ouverture aux autres.

Cette proposition de culture de la sécurité repose sur un recadrage—sur le passage de la peur à l'assurance, de l'aversion au risque au courage, de l'isolement aux liens, et de la suspicion à la confiance.

Il est logique d'avoir peur—l'État est très puissant, la répression est fréquente et elle a le pouvoir de nous écraser, nous et tous nos projets. Mais je ne veux pas être paralysée par cette peur. Avec des informations précises et un bon plan, on peut commencer à transformer la peur en **assurance**, en sachant qu'on a des pratiques de sécurité à la hauteur des risques auxquels on fait face. En fait, sans transformer la peur, il est difficile d'imaginer comment même agir face au pouvoir de nos ennemis.

Je ne veux pas avoir peur du risque. Je veux faire le choix de mes actes en fonction de leur efficacité, de leur pertinence, de mon analyse et de mon éthique. Une bonne culture de la sécurité nous permet de faire preuve de **courage** dans nos tactiques collectives, car on sait qu'on peut gérer les risques. Lorsqu'on ne transforme pas l'aversion au risque, on s'auto-police et on reste confiné à l'espace d'opposition symbolique qui nous est fourni.

La répression fonctionne en isolant les gens. Je ne veux pas contribuer à cet isolement par ce que je fais pour ma sécurité et celle de mes ami·e·s. Je veux une culture de la sécurité enracinée dans l'approfondissement de nos **liens** les un·e·s avec les autres. Quand on ne dépasse pas l'isolement, l'or-

ganisation risque de ressembler au travail et de ne pas permettre le genre de relations qui nous transforment vraiment, d'une manière qui nous fait ressentir le monde que nous voulons créer.

Je ne veux pas me méfier des gens que je rencontre. C'est toxique et ça désagrège les espaces de lutte qu'on crée. Plutôt que de ressentir de la méfiance envers quelqu'un, je préfère me demander : « Qu'est-ce que ça prendrait pour que je fasse **confiance** à cette personne ? » Je veux aller vers les gens et essayer de transformer la méfiance en confiance.

Je voudrais proposer une définition de la culture de la sécurité pour donner une perspective à cette conversation. **La culture de la sécurité est un ensemble de pratiques développées pour évaluer les risques, contrôler les flux d'informations dans nos réseaux, et construire des relations de lutte fortes.** Il existe d'innombrables cultures de la sécurité possibles, mais ce qui est important c'est qu'elles viennent de discussions claires et explicites à propos des risques et s'adaptent au changement. Dans l'exemple qui suit, le rapport au risque s'adapte à l'évolution des actions et à la répression. Les pratiques de culture de la sécurité qui y sont mentionnées seront expliquées plus loin.

> Dans une mobilisation contre un oléoduc, là où je vis, on a voulu mettre l'accent sur les actions directes de masse visant les infrastructures pétrolières. On a établi que, pour les premières étapes de cette mobilisation où on se concentrait sur la sensibilisation et la recherche, le risque qu'on courait était très faible et qu'on pouvait en toute sécurité faire participer de nombreuses personnes à ces étapes, et partager ouvertement les infos par n'importe quel moyen. Quand on a commencé à planifier des actions symboliques, cette considération n'a pas beaucoup changé, mais quand on a commencé à planifier des choses comme bloquer des routes ou manifester devant un commissariat, l'élément de surprise est devenu une considération plus importante. En dehors des risques pénaux encourus, nos actions seraient tout simplement moins efficaces si elles étaient connues à l'avance. On a donc cessé d'utiliser des moyens de communication publics ou facilement surveillés et on a commencé à demander que les gens ne communiquent les détails qu'à des personnes de confiance ayant l'intention de participer.
>
> Peu après le début de cette phase de la mobilisation, un dispositif policier national appelé Joint Intelligence Group (JIG) s'est formé pour défendre les oléoducs, avec la participation de différents services de police et de renseignement. Les JIG et les dispositifs de ce genre

sont de plus en plus courantes en Europe et en Amérique du Nord ces dernières années.

Ma **proposition pour les réseaux sociaux** est la suivante. Privilégier les rencontres en face-à-face. Se rencontrer régulièrement si possible, ainsi le prochain rendez-vous est déjà prévu au cas où la communication en ligne soit perturbée. Quand on utilise les réseaux sociaux, demandons-nous si c'est vraiment nécessaire si c'était possible d'utiliser un autre moyen de communication. Je vous encourage à voir un réseau social comme un mégaphone, une façon d'amplifier votre voix. Ce n'est pas comme dans un salon où on discute et on apprend à connaître les gens. Utilisez ces réseaux pour promouvoir, annoncer, disséminer, mais ayez vos conversations ailleurs. Dans les luttes auxquelles je participe, on efface presque tous les commentaires des pages qu'on administre et on les déplace vers d'autres plateformes dès qu'on les reçoit. On utilise des comptes partagés quand c'est possible et on limite notre dépendance aux comptes liés à des informations personnelles. Peut-être que vous ne voulez pas aller aussi loin, peut-être que vous voulez aller plus loin, mais c'est en tout cas une façon d'utiliser la puissance des réseaux sociaux tout en évitant leurs principaux désavantages.

L'évolution de nos usages des réseaux sociaux peut se faire graduellement, en observant ces usages de manière critique et en les déplaçant petit à petit vers d'autres platformes, ou mieux, en les transformant en rencontres en face-à-face. Ça a pris du temps pour que tant d'aspects de nos vies soient capturés par ces entreprises dégueu, et développer de nouvelles habitudes et cultures de luttes qui résistent à ces entreprises nous prendra peut-être beaucoup de temps aussi.

Enfin, parlons un peu de **sécurité informatique**[8]. Le sujet est complexe et c'est facile de s'embourber. Néanmoins, il y a quelques règles simples que l'on peut suivre pour améliorer notre sécurité informatique. Voici trois points.

Un : Utilise le chiffrement de bout en bout à moins que tu aies une raison de ne pas le faire. Cette technologie peut être compliquée, mais de nos jours

[8] *NdNTP :* Pour d'autres conseils de sécurité numérique, voir notre Threat Library[9].
[9] https://notrace.how/threat-library/mitigations/digital-best-practices.html

propres limites. Ce genre de désarmement préventif est une vraie position de faiblesse.

Sur de telles plateformes, on prend aussi le risque d'être *submergé de réactions hostiles*. On ne peut pas contrôler comment nos actions seront reçues, et parfois nos actions ne sont pas très populaires—après tout, on veut un monde sans capitalisme organisé sur des bases radicalement différentes. Les réactions sur Internet après une action impopulaire peuvent être déstabilisantes. Lors d'une récente mobilisation antifasciste dans ma ville, l'extrême-droite et les médias de masse ont réussi à provoquer un contrecoup contre les antifascistes qui a inondé les réseaux sociaux de menaces et de colère. Les antifascistes dépendaient fortement de Facebook pour s'organiser et iels ont dû faire face à un choix : rester hors ligne et éviter le contre-coup, mais être isolés de leurs camarades ou aller en ligne et discuter avec les gens, mais en ayant des conversations dominées par le stress et l'hostilité. Cette dynamique rend la lutte moins résiliente et notre travail plus perturbable par la mauvaise presse.

Le *contrôle des plateformes par les entreprises* est un autre problème. Facebook est une entreprise énorme et riche dont les intérêts sont opposés aux nôtres—ce qui est bon pour nous est mauvais pour elle. Si on dépend de ses infrastructures, elle est capable de nous faire taire à n'importe quel moment pour n'importe quelle raison. De telles entreprises sont très sensibles à la pression du public. On n'a pas besoin de réfléchir longtemps pour trouver des exemples de projets qui sont devenus impopulaires et qui ont perdu leurs pages et ainsi, leur capacité à communiquer avec leur base. Si on est trop dépendants de ces entreprises, ça peut être un désastre. Demandez-vous ce que vous feriez si toutes vos pages et vos comptes disparaissaient ce soir—comment est-ce que vous vous organiseriez demain ?

Il y a aussi le problème de la *surveillance*, qui ne devrait pas être controversé. Tout ce qui est écrit sur Facebook est sauvegardé pour toujours dans une base de données à laquelle la police peut avoir accès en tout temps. Facebook (tout comme Google et d'autres) vous traque et espionne vos appareils. Ces données sont également accessibles aux agences de renseignement et de sécurité. Ce n'est pas une théorie, ça a été prouvé à maintes reprises, et des accusations contre des militants basées sur ces données

> constituent une menace spécifique envers les luttes de toutes sortes, car ils visent directement à perturber les luttes et disposent d'importantes ressources. Donc, même si nos actions n'ont pas changé, on a repensé notre rapport au risque et on a décidé d'isoler les organisateur·ice·s des actions de possibles accusations de conspiration en planifiant les actions au sein d'un petit groupe opaque. On pouvait inviter à participer des personnes en qui on avait confiance, et on pouvait prendre des mesures pour établir cette confiance, comme vérifier les identités les uns des autres. Mais on ne planifierait plus les actions ouvertement au niveau du réseau plus large de personnes intéressées par le travail de sensibilisation. Grâce à ce changement, quand on s'est orienté vers le sabotage d'infrastructures critiques, il nous a suffi d'élargir le noyau qu'on avait formé et d'encourager d'autres groupes à s'organiser de la même manière. La coordination des groupes (groupes passés par un *vouching*, voir ci-dessous) se faisait via des réunions rassemblant des représentant·e·s de chaque groupe, où le rôle de chacun était décidé.

(Ce modèle d'organisation, comme tous les autres modèles, vient évidemment avec ses forces et ses faiblesses. Mon intention dans ce texte n'est pas de faire l'apologie d'une manière de s'organiser en particulier, bien que j'aie plus d'expérience avec certaines qu'avec d'autres.)

Avant d'approfondir des idées et des pratiques spécifiques, je veux parler d'une objection courante que les gens ont à l'égard des discussions sur la culture de la sécurité dans leur lutte : « **Je ne fais rien d'illégal donc je n'ai pas besoin de penser à la sécurité** ». Ou alors plus spécifiquement, mais l'objection sous-jacente est la même : « Je ne parle de rien d'incriminant, inutile de me préoccuper de la surveillance », ou « En général, je ne me fais pas arrêter à la frontière, donc je n'ai pas à me soucier des tas de brochures anarchistes dans ma voiture ».

C'est l'État et nul autre qui décide de réprimer ou de saper les luttes—ce qui ne passe pas forcément pas la criminalisation d'actions spécifiques. Personnellement, j'ai eu un certain nombre de condamnations pénales : j'ai passé environ un an en prison, deux ans en détention à domicile, et à peu près cinq ans avec diverses restrictions de liberté. Toutes ces condamnations étaient pour des activités de lutte de routine que l'État a choisi de réprimer pour des raisons qui lui sont propres. J'ai été condamnée à huit mois de prison pour avoir aidé à organiser des réunions et pour avoir écrit et distribué un appel à une manifestation lors d'un contre-sommet ;

quelques années plus tard, j'ai été condamnée à un an pour avoir distribué un tract annonçant une manifestation et y avoir ensuite participé. Dans ces deux cas, il y a eu des dégâts matériels lors des manifestations, mais je n'en ai jamais été accusée. L'État a plutôt choisi d'utiliser des accusations de conspiration pour cibler des gens s'organisant de manière visible et routinière comme je l'ai fait à maintes reprises. Une dynamique similaire s'est manifestée dans d'autres affaires de conspiration aux États-Unis et au Canada. Mon expérience n'a rien d'exceptionnel.

Je ne raconte pas ça pour me positionner comme victime—je veux m'organiser pour menacer le pouvoir, donc il me semble logique d'être ciblée pour ça. Ce qui est notable, c'est que l'État choisisse de criminaliser la distribution de tracts et l'organisation de réunions afin d'intimider ou de faire des exemples. Même si ce genre de répression ne se produisait que dans 1% des cas (bien que ça semble arriver plus souvent), on doit faire attention et s'organiser en conséquence avec des pratiques de sécurité adaptées. Sinon on aura plus d'autre choix que de préventivement restreindre nos activités, intérioriser la répression et intégrer la crainte et la faiblesse à nos pratiques.

Ceci dit, la culture de la sécurité ne consiste pas seulement à se protéger des accusations pénales. Il s'agit d'empêcher que nos activités soient perturbées. La criminalisation est une menace particulière, mais c'est loin d'être la seule.

Pendant le contre-sommet où j'ai été accusée de conspiration, seuls deux des seize infiltré·e·s du JIG étaient impliqués dans le procès lui-même. Les autres avaient changé des mots de passe de sites Web et d'adresses électroniques, dirigé des autobus vers les mauvais endroits, volé du matériel médical, répandu des rumeurs pour aggraver certains conflits, et même tenté de piéger des jeunes dans un étrange complot autour d'un attentat à la bombe. Toutes ces actions policières ont eu un effet extrêmement perturbateur, sans jamais avoir besoin de recourir au pouvoir des tribunaux, et on ne connaîtra sans doute jamais l'étendue de leur impact.

On a déjà vu que le maintien de l'élément de surprise est souvent une considération importante en matière de sécurité. Un exemple dans notre région est l'organisation de manifs devant des prisons en soutien aux personnes à l'intérieur : en les organisant discrètement, on peut avoir une

rale de leurs organisations plutôt que comme un moyen de les renforcer. Certaines des pratiques ci-dessus ne s'appliquent peut-être pas aux organisations de masse formelles, mais j'argumenterais que tous les principes généraux s'appliquent. En fait, je crois que si de telles organisations font attention à leurs modes de fonctionnement, elles verront certaines de ces pratiques y existent déjà.

Par exemple, dans les sections du IWW, il est fréquent de s'organiser en secret au sein d'un lieu de travail. Parfois des noms de code sont utilisés, et seules des informations générales sont rendues publiques. Il est aussi fréquent pour de telles organisations d'assigner des petits comités à certaines tâches comme l'organisation d'une manif, et les réunions de ces comités ne sont pas forcément ouvertes aux personnes non-impliquées, ou bien des moyens de communication spécifiques sont utilisés pour éviter les grosses listes mail et les réseaux sociaux.

Ce que je suggère, c'est que des conversations explicites à propos des risques et de la sécurité soient incorporées dans les différents projets menés par ces organisations. La formation de comités autonomes qui décident de leurs propres pratiques de sécurité est une étape importante, tout comme accueillir des initiatives individuelles par des membres qui s'associent sur des bases affinitaires. C'est-à-dire que la structure doit être assez flexible pour accommoder différentes formes d'organisation pour différents types d'activité.

Certaines objections à la culture de la sécurité viennent souvent de celleux qui utilisent des réseaux sociaux comme le populaire Facebook. J'aimerais apporter quelques **critiques de l'organisation par Facebook** et proposer une manière pour les grosses organisations qui en dépendent de faire autrement.

Le point crucial est que les réseaux sociaux contrôlés par des entreprises *réduisent les possibilités* d'organisation. Puisque s'organiser par ces réseaux est à peu près aussi privé que de s'organiser dans la salle d'attente d'un commissariat (chose qui est largement admise de nos jours), il y a des limites strictes à ce qui peut y être discuté. Ce qui veut dire que si on est dépendants de Facebook parce que c'est notre principal moyen d'organisation, les limites de ce qui peut être pensé et planifié deviennent nos

brisé les « Deux Jamais »), il arrivait à détourner ces préoccupations en répondant qu'ils étaient racistes envers lui. Il a trouvé du soutien chez un groupe d'activistes antiracistes dans une autre communauté que celle qu'il ciblait principalement et il a réussi à résister à plusieurs tentatives pour l'expulser des espaces d'organisation. Il a fini par témoigner dans un dossier qui a envoyé six personnes en prison. Il a certainement vécu du racisme dans notre milieu, ce qui, combiné à sa manipulation cynique de l'antiracisme, devrait nous pousser à examiner les faiblesses de nos politiques antiracistes. Avoir des politiques claires sur le racisme, les oppressions de genre et d'autres oppressions (c'est-à-dire être à l'aise de discuter de nos analyses sur ces sujets) ainsi que des pratiques pour adresser ces sujets de front quand ils surviennent peut réduire les chances de réussite de telles stratégies d'infiltration.

Il peut y avoir plein de raisons de ne pas faire confiance à quelqu'un, et plein de comportement prédateurs qui n'impliquent pas qu'une personne soit un flic infiltré. Le cas de Brandon Darby en est un exemple. Dans le texte « Pourquoi les misogynes font des super indics[6] », les auteur·ice·s affirment que les gens auraient dû faire plus d'efforts pour aborder les comportements très sexistes de Darby avant même qu'il commence à coopérer avec le FBI[7] et qu'il piège plusieurs personnes. Darby est un exemple extrême, mais il arrive très souvent dans notre milieu que des gens se sentent mal à l'aise à cause de comportements patriarcaux. Parfois, les gens vont développer des soupçons envers ceux qui ont ces comportements, ce qui est compréhensible, mais c'est une erreur de chercher des infiltrés lorsque ce qui est devant nos yeux, c'est du sexisme : les comportements destructeurs doivent être abordés en tant que tels. Et si ça nous aide contre des indics comme Darby, tant mieux.

Un mot sur les **organisations de masse** formelles. Ces organisations sont souvent imperméables aux débats sur la culture de la sécurité car elles associent ces débats à des modes d'organisation qui ne leur correspondent pas. La culture de la sécurité peut être perçue comme une critique géné-

[6] https://notrace.how/resources/fr/index.html#why-misogynists-make-great-informants

[7] *NdNTP :* Federal Bureau of Investigation, le principal service fédéral de police judiciaire et de renseignement intérieur aux États-Unis.

liberté de mouvement et d'action pendant un certain temps avant que la police ne soit en mesure d'intervenir. Ou imaginons qu'une section de l'IWW[1] tente de lancer une mobilisation de type « Réclame ta paye » contre un patron—iels devront prendre des mesures pour se protéger contre des poursuites au civil ou le risque d'être ciblé·e·s par une entreprise de sécurité privée. Ou bien prenons le travail que font les antifascistes pour identifier l'extrême-droite—iels doivent se prémunir contre la divulgation de leurs propres informations personnelles et contre les violences dont iels pourraient faire l'objet dans la rue. Il y a aussi de plus en plus d'entreprises de sécurité privées engagées pour défendre des intérêts privés (et celles-ci peuvent faire des choses que la police ne peut ou ne veut pas faire), ce qui est arrivé à plusieurs reprises ces dernières années dans les luttes de défense de terres menées par les autochtones.

Les préoccupations en matière de sécurité sont déjà en grande partie intégrées dans nos modes d'organisation. Pour bâtir une culture de la sécurité, il faut évaluer les risques de manière explicite au-delà de quelques actions spécifiques, et adopter des pratiques claires conçues pour nous garder en liberté et assurer l'efficacité de nos actions, quelles que soient les formes que prennent nos luttes. Pour ça, il faut se concentrer sur la mise en place de liens solides, tout en créant un climat de confiance où il est possible d'agir avec assurance.

Voici selon moi quelques **principes de base** de culture de la sécurité :

Les « Deux Jamais ». Même s'ils sont relativement bien connus, ces deux points sont aussi un peu inadéquats. Dans leur forme a plus simple, ils sont : « Ne jamais parler de sa propre implication dans une activité illégale. Ne jamais parler de l'implication de quelqu'un d'autre dans une activité illégale. »

Mais c'est inadéquat, parce que la majorité de ce qu'on fait n'est pas clairement illégal. On pourrait donc reformuler les « Deux Jamais » comme : « Ne jamais parler de sa propre implication ou de l'implication de quelqu'un d'autre dans une activité qui risque d'être criminalisée. Ne jamais parler de l'intérêt de quelqu'un d'autre pour une activité criminalisée. »

[1] *Note du No Trace Project (NdNTP) :* Industrial Workers of the World, un syndicat international fondé aux États-Unis en 1905.

Mais cette reformulation est encore inadéquate, parce que les accusations pénales ne sont pas le seul risque. Bien sûr, avoir une règle claire et respectée par tou·te·s de ne pas parler inutilement de trucs illégaux est une bonne idée, peu importe où on se trouve. Ça inclut ce qu'on croit parfois être des blagues—des paroles en l'air à propos de combattre les flics ou d'attaquer la propriété privée peuvent sembler moins légères lorsqu'elles sont consignées dans le rapport d'un infiltré.

L'une des raisons courantes qui font qu'on se met à douter d'une personne c'est quand cette personne essaie de prendre des gens à part pour discuter de tactiques illégales. Plutôt que de dire : « Cette personne est un flic qui tente de me piéger », on peut reformuler nos propos et dire : « J'ai besoin de clarifier ma vision de la culture de la sécurité avec cette personne si on continue à travailler ensemble ». La version reformulée des « Deux Jamais » peut permettre cette clarification. Elle nous aide aussi à nous souvenir de ne pas spéculer sur qui est à l'origine d'actions anonymes accomplies autour de nous. Ça, c'est le rôle de la police. Si autour de nous, des gens se demandent qui sont derrière des actions illégales anonymes, on peut leur rappeler simplement que l'action a été faite anonymement, que ce n'est pas important de savoir qui l'a faite et que l'action parle d'elle-même.

(Une chose dont on parle moins est comment les reproches autour de la culture de la sécurité peuvent renforcer des dynamiques de pouvoir néfastes. On doit absolument parler entre nous des interactions qui nous posent problème en terme de sécurité, mais ça devrait toujours être mutuel et fait en privé si possible—décris ce que tu as entendu, présente ton idée de culture de la sécurité, demande si l'autre pense que c'est une limite raisonnable, sois prêt·e à écouter son désaccord. L'objectif est de construire une compréhension partagée pour élargir les formes d'organisation dans lesquelles on peut s'engager ensemble, pas que les autres se sentent honteux (ni se sentir soi-même plus *hardcore*). Une forme encore plus extrême de ça est de faire courir des ragots comme quoi quelqu'un·e serait un·e informateur·trice sans preuve à l'appui, ce qui peut avoir d'importantes conséquences sur la vie des gens ; ça a été une des causes de l'éclatement des mouvements révolutionnaires des années 1970. Un moindre exemple peut être qu'une personne plus « expérimentée » en rabaisse une autre de-

est très facile d'initier des projets avec des degrés de risques variés, chacun avec sa culture de la sécurité adaptée. Cela implique aussi qu'il n'y ait que les gens concernés qui connaissent les détails ou les personnes impliquées, à moins qu'il en soit décidé autrement.

Une flexibilité semblable peut être incorporée dans d'autres modèles d'organisation. La clé est de respecter et de légitimer les initiatives individuelles, en n'exigeant pas que chaque activité soit approuvée par une entité centralisée. Une autre clé est le respect de la liberté d'association : considérer comme normal de travailler en petits groupes choisis aux côtés de groupes plus larges ayant des structures plus ouvertes. Ça peut ressembler à des comités ou à des groupes de travail ayant la capacité de définir leurs propres critères de participation. Ça peut aussi être d'être ouvert à certains éléments de l'organisation affinitaire décrite plus haut ou d'être explicite quant à quelles informations partager à qui.

Enfin, **aborder les mauvaises dynamiques de façon proactive** est généralement une bonne habitude à avoir, mais c'est si important en terme de sécurité qu'on devrait insister dessus dans chaque conversation sur la culture de la sécurité. De nombreuses dynamiques peuvent éroder la confiance et rendre l'organisation plus difficile. Par exemple le *bullying* (harcèlement, brimades), ou les comportements oppressifs enracinés dans le patriarcat ou la suprématie blanche. Un autre exemple est la centralisation des ressources et des contacts, qui fait que les projets ne peuvent être initiés que par certaines personnes. Ou encore de dire du mal des autres dans leur dos, de se vanter, ou de briser les « Deux Jamais » en posant des questions à propos des activités criminelles d'autrui. Quiconque ayant été impliqué dans un milieu militant peut facilement lister les mauvaises dynamiques qui s'y trouvent.

Comme je l'ai dit plus haut en parlant des difficultés liées à la vérification d'identité, nos difficultés liées aux mauvaises dynamiques et à l'oppression dans nos milieux sont des points faibles que la police et le renseignement connaissent de plus en plus. J'ai mentionné la flic qui prétendait fuir une relation abusive pour s'immiscer dans la vie des gens (elle avait même intégré la coloc d'une personne). Une autre expérience d'infiltration impliquait un flic dans la quarantaine à la peau foncée. Lorsque les gens parlaient de comment celui-ci les mettait mal à l'aise (entre autres pour avoir

Les **cercles de confiance** sont surtout destinés aux réseaux informels et à l'organisation sur des bases affinitaires (ce qui correspond à la plupart de mes expériences d'organisation). Cette technique consiste à écrire les noms des individus dans votre réseau autour d'un cercle puis à tracer différents types de lignes entre ceux-ci pour symboliser les types de relations qu'ils ont entre eux. Une ligne continue pourrait représenter une relation forte et basée sur la confiance. Une ligne brisée pourrait signifier un certain niveau de confiance et une ligne pointillée que vous ne vous connaissez pas bien. Ce processus collaboratif peut en dire long sur les dynamiques de groupe et visibiliser les liens qu'il faudrait renforcer pour développer de la confiance[5].

Ça peut révéler que seule une personne a des relations fortes avec tout le monde et que les autres liens sont moins solides. Cela voudrait dire qu'il y a un travail à faire pour équilibrer le réseau, ce qui le rendrait aussi plus résistant (au cas où cette personne est arrêtée ou simplement tombe malade ou fait un *burn out*) et plus égalitaire, car la capacité à lancer des projets est liée au nombre de personnes qui font confiance à la personne qui les lance. Cet exercice peut également montrer qu'il y a quelqu'un en qui personne ne fait confiance.

Souvent, un infiltré se rapproche d'un premier milieu, puis utilise les noms des contacts établis au sein celui-ci pour se rapprocher d'un deuxième milieu. Le *vouching* et les cercles de confiance protègent bien contre ça. Au-delà de démasquer les individus hostiles, les cercles de confiance nous permettent de renforcer nos réseaux en transformant ces lignes brisées en lignes continues autant que possible.

Les **structures organisationnelles flexibles** permettent à nos luttes de s'adapter aux besoins de différents types d'activité. L'organisation informelle sur des bases affinitaires est un modèle développé pour répondre à ce besoin. Dans un réseau informel (c'est-à-dire sans structure fixe), les individus communiquent leurs idées et leurs intentions puis des groupes affinitaires se forment autour d'un projet quelconque ou d'un désir partagé d'intervenir sur des bases communes. La force de ce modèle est qu'il

[5] *NdNTP :* Après avoir réalisé cet exercice, nous conseillons de détruire immédiatement détruire le support utilisé pour l'exercice pour ne pas que les flics tombent dessus un jour.

vant un groupe pour avoir parlé d'actions qu'iel a trouvé inspirantes ou parce qu'iel parle aux mauvaises personnes.)

Un autre principe de base est de **privilégier les rencontres en face-à-face**. Peu importe la sécurité de tel ou tel outil de communication, on construit une meilleure confiance, des relations plus solides et on prend de meilleures décisions quand on prend le temps de se rencontrer en personne. Quand les outils de communication électroniques remplacent le face-à-face, nos conversations sont plus faciles à surveiller, génèrent plus de malentendus, et peuvent être perturbées par des décisions ou des problèmes liés aux entreprises qui gèrent ces outils. Chaque fois que tu utilises des outils électroniques pour t'organiser, demande-toi si cela remplace les rencontres face à face. Si c'est le cas, demande-toi si c'est vraiment nécessaire. Envisage de réduire ta dépendance à ces outils. (On reviendra un peu plus loin sur la sécurité informatique…)

Une des objections à ça est que plein de gens ont de l'anxiété sociale et préfèrent communiquer via leurs appareils ; une autre est que se déplacer physiquement est impossible pour certaines personnes. Comme pour d'autres sujets difficiles qui émergent quand on parle de culture de la sécurité, je t'encourage à faire face à ces obstacles et à chercher d'autres moyens de satisfaire ces besoins en essayant tout de même de prioriser les rencontres en face-à-face. Après tout, ces technologies sont très récentes et les gens ayant des handicaps de toutes sortes ont depuis longtemps développé des moyens pour se retrouver et s'organiser autour de sujets qui les affectent.

La répression est inévitable, essayer de l'éviter à tout prix ne vaut pas la peine. Peu importe la lutte, si elle est menée au-delà des limites de la légalité, elle deviendra une lutte contre la police, dont le rôle est de défendre ce monde tel qu'il est. Si on part avec l'idée que l'on évitera la répression à tout prix, on n'utilisera que des formes de luttes approuvées par la police, ce qui rend quasi impossible la construction d'un pouvoir collectif capable d'un changement transformateur. Pour ne pas subir ces limites, on doit être prêt·e·s à faire face à la répression.

Une façon de s'y préparer est de mettre la police et les prisons au centre de nos luttes dès le départ. Là-dessus, on peut apprendre des mouvements antiracistes qui gardent toujours en tête la violence raciste et physique de

ces institutions et cela même lorsqu'ils choisissent de se concentrer sur des sujets plus larges. L'avantage c'est qu'on construit une culture de lutte qui n'est pas choquée par la violence policière et qui est réaliste quant à la prison. On peut aller un peu plus loin et incorporer des pratiques de solidarité dans nos luttes. Si on s'organise sur un lieu de travail on peut s'intéresser aux luttes de travailleur·euse·s ailleurs et réfléchir à des actes de solidarité pratiques avec celleux qui font face à la répression. Si on s'organise autour des questions queer on peut trouver et soutenir des prisonniers queers, et au passage apprendre à connaître les prisons de la région au cas où ça nous soit utile un jour. Si on s'intéresse aux luttes écolo et de défense de terres, il y a des défenseur·e·s de terres en prison qui font face à des accusations et à la violence physique de l'État à travers tout le continent ; incorporer des pratiques de solidarité avec elleux dans nos projets peut donner une puissante inspiration en vue d'une résistance forte et courageuse.

Un autre avntage est qu'on recevra sans doute plus de solidarité en retour puisque la prison est une grande force unificatrice qui relie toutes les formes de luttes contre la domination et l'oppression. Prendre part à une culture de résistance qui démontre de la solidarité active face à la répression peut jouer gros dans le fait de nous garder en sécurité. Comme toujours, c'est en ayant de bonnes informations qu'on combat la peur. Plus on en sait à propos du fonctionnement de la police et des prisons, plus on peut transformer notre peur en préparation et en confiance en nous-même.

Avec ça en tête, observons plus en détail **ce que signifie évaluer les risques**. Ce qui importe ici est de le faire ouvertement et régulièrement puis de se focaliser sur comment rendre possibles les actions qu'on pense efficaces et appropriées. Ça peut être facile d'être dans un état d'esprit réticent au risque et de s'auto-policer encore plus de ce que l'État arrive à nous contrôler. Être explicites quant aux risques peut faire en sorte que ce soit plus facile de mettre l'accent sur le courage et les possibilités.

Si vous vous posez pour prévoir une manif, pensez au ton qu'elle prendra. Est-ce que vous l'imaginez calme et ordonnée ? Ou combative et incontrôlable ? Si la police tente de vous bloquer, est-ce que vous resterez passifs où est-ce que vous essaierez de leur rentrer dedans ? Est-ce qu'il y a des actions que vous seriez excités de voir advenir pendant la manif, mais qui

systématique. La première étape est d'avoir des bases de confiance claires au sein d'un groupe. La base de confiance peut être que les membres aient des idées compatibles et soient fiables. Ou alors de s'assurer que les membres sont bien ceux qu'ils prétendent être, qu'ils ne paniquent pas en cas de stress, qu'ils ont certaines expériences d'organisation et qu'ils sont à l'aise avec certains types d'actions. Peu importe cette base, le *vouching* c'est quand un ou plusieurs membres existants introduisent une nouvelle personne au groupe, et affirment que celle-ci correspond aux bases de confiance du groupe. Les autres membres doivent explicitement accepter ou rejeter ce *vouch*. L'aspect explicite du *vouching* évite le risque de faire implicitement confiance aux gens pour des raisons superficielles, par exemple parce qu'ils correspondent aux normes culturelles d'un milieu, parce qu'on présume de leur personnalité, ou parce qu'on présume que d'autres personnes leur font confiance.

Voici un exemple de *vouch*, c'est-à-dire d'assurances données par des membres existants du groupe vis-à-vis d'une nouvelle personne :

> « Je connais cette personne depuis cinq ans, durant ce temps on a travaillé ensemble sur des projets publics et je lui fais confiance pour me soutenir dans des moments difficiles. Je suis allé dîner chez son père une fois et je suis souvent allé la chercher au travail. »

Voici un autre exemple :

> « J'ai rencontré cette personne l'an dernier à un événement sur le changement climatique et on s'est vu plusieurs fois à des événements écolos depuis. On a souvent discuté de différents sujets et je l'aime bien. Je sais qu'elle cherche à gagner en expérience dans l'organisation d'actions et je crois que ça pourrait fonctionner avec nous. »

Une exception au fait d'être explicite sur les raisons qu'on a de faire confiance à quelqu'un est de ne pas briser les « Deux Jamais ». Si vous organisez des actions clandestines, inviter de nouvelles personnes ou présenter un groupe à un autre est délicat : le *vouching* reste une bonne idée mais il est important de ne pas parler des actions auxquelles une personne a participé afin de ne pas la mettre en danger. Comme il est nécessaire d'avoir une forte base de confiance pour faire ce type d'actions, il est possible de faire confiance au jugement de quelqu'un sans demander de détails d'actions spécifiques.

l'autre bout du fil donner des détails sur la vie ou le travail de la personne. D'autres fois, la pièce d'identité était suffisante. Parfois on s'est montré nos appartements respectifs. L'idée était que ce soit aussi mutuel que possible (ce qui est difficile, car en pratique, il y a toujours une personne qui initie le processus) et de se concentrer sur la construction de la confiance.

C'est inutile de faire de telles vérifications d'identité avec des personnes en qui on n'a pas confiance ou avec qui on ne se sent pas à l'aise de faire des actions risquées. Le but n'est pas de démasquer des flics mais d'approfondir notre confiance et notre assurance. Vérifier nos identités de cette façon devrait être un signe de respect.

Plusieurs facteurs peuvent venir compliquer ce processus. Par exemple, les gens qui ont immigré n'ont peut-être pas de famille à proximité ou le même type de documents. Souvent, les personnes queers et trans n'utilisent pas les noms inscrits sur leurs documents officiels et iels ne se sentent peut-être pas à l'aise de partager leurs noms légaux ou de vielles photos. Néanmoins, ce sont des éléments à prendre en compte et auxquels s'adapter, pas des raisons de faire des exceptions. Une flic infiltrée dans ma région prétendait fuir une relation abusive et a utilisé les pratiques de solidarité avec les survivant·e·s d'agression pour éviter de parler des détails de son passé. Notre inconfort quant aux sujets plus sensibles et complexes crée des angles morts qui peuvent être utilisés par celleux qui nous veulent du mal—on doit être courageux et trouver les moyens d'aborder cette complexité. On ne doit pas l'éviter.

Un·e ami·e qui a expérimenté les vérifications d'identité pense qu'il y a peut-être des moments où c'est OK d'être moins mutuel, lorsqu'on ne veut pas donner aux gens trop de contrôle sur le type de preuve à apporter. Iel met aussi l'accent sur le fait que les vérifications d'identité n'aident pas forcément dans le cas des balances (en opposition aux infiltrés) qui sont bien celleux qu'iels prétendent être, mais qui ont de mauvaises intentions. Il faut aussi prévoir quoi faire si quelqu'un ne peut ou ne veut pas jouer le jeu, ou si on découvre quelque chose qui nous fait ré-évaluer la confiance qu'on avait en la personne.

Le **vouching** est une technique pour intégrer de nouvelles personnes dans un groupe déjà existant ou dans un espace d'organisation. Tout comme nos autres pratiques, c'est mieux lorsque c'est explicite et fait de manière

risquent d'être criminalisées plus que le défilé en lui-même ? Ça peut être aussi basique que de poser des autocollants ou bien ça peut être de faire des tags ou de briser des vitrines. Est-ce que votre plan sera menacé si vous perdez l'élément de surprise ? Qui ne doit pas être mis au courant de ce plan ? Comment est-ce que vous allez joindre les personnes que vous devez contacter sans risquer que les mauvaises personnes aient vent de l'initiative ? Communiquer clairement à propos du ton que prendra une action peut aider les autres à élaborer des plans autonomes appropriés.

C'est important d'éviter le laisser-aller et de ne pas prendre les choses pour acquis. Voici un exemple de 2018 :

> Les organisateur·trice·s d'un salon du livre anarchiste ont décidé d'appeler à une manif de nuit après l'événement. Iels avaient mis beaucoup d'énergie dans les autres aspects de la journée et ont négligé les risques de la manif, parce qu'iels avaient organisé un tas de manifs auparavant. Néanmoins, la manif a été beaucoup plus combative que toutes les autres et il y a eu beaucoup de dégâts matériels—iels n'avaient pas évalué explicitement les risques alors que l'heure du rendez-vous approchait. Iels n'avaient pas non plus pris en compte que le JIG se focalisant sur un sommet du G7 qui allait avoir lieu dans une autre province cet été-là, ça pouvait faire que des ressources policières additionnelles les cibleraient durant cette période. Du coup les pratiques de sécurité dans l'organisation de la manif n'étaient pas adaptées aux risques que l'action a fini par comporter et tous les organisateurs du salon du livre ont été accusé·e·s de conspiration.

Il s'agit d'un exemple extrême, mais des imprévus vont toujours advenir et c'est généralement une bonne chose, vu qu'on ne peut pas vraiment prévoir notre chemin vers les situations insurrectionnelles. Rester actif·ve dans notre évaluation des risques peut réduire les chances d'être pris par surprise. Mettre régulièrement en pratique une culture de la sécurité rigoureuse peut limiter les dégâts dans ce genre de situation. Dans cet exemple, une bonne sécurité informatique, une culture de non-coopération avec la police, une solidarité persistante et active, une bonne dissimulation des visages, et un refus d'abandonner ou de se soumettre ont fait que cette situation inattendue s'est avérée bien moins problématique qu'elle aurait pu l'être, et les peronnes ont surmonté la situation la tête haute.

Comme autre exemple, prenons le développement d'une organisation de masse, par exemple une organisation antifasciste. Quel genre de questions doit-on se poser pour évaluer les risques, même si aucune mobilisation n'est prévue ? De quel niveau de confiance a-t-on besoin entre nous par rapport au genre de choses que l'on veut faire ? On risque peut-être d'être infiltré par la police donc savoir qu'on est tou·te·s les personnes qu'on prétend être peut être important. On pourrait aussi être infiltré par l'extrême droite, auquel cas comprendre nos lignes politiques respectives et construire graduellement une confiance mutuelle via des actions qui augmentent doucement en intensité peut être une solution. Le principe de privilégier les rencontres en face-à-face plutôt que la communication en ligne rendra sans doute ces objectifs plus atteignables.

Si le but est de développer les actions pendant les manifs alors il est possible de discuter de discipline et de planification. Quelles sont les attentes des un·e·s envers les autres dans des situations tendues ? Il est difficile de respecter des attentes lorsqu'elles sont vagues, et plus facile d'agir intelligemment quand on a un plan clair et qu'on arrive à estimer si ce plan fonctionne ou pas. Développer de bonnes habitudes pour gérer des situations au sein d'un groupe a d'énormes conséquences en terme de sécurité lors des manifs—ce n'est pas la culture de la sécurité, mais c'est assez lié. Par exemple, les risques des manifs antifascistes peuvent inclure d'être trop peu nombreux·ses, être encerclé·e·s ou séparé·e·s, être suivi·e·s ou identifié·e·s par l'extrême droite ou par la police, subir des blessures inutiles ou se faire arrêter.

Quelques pratiques qui tiennent compte des risques lors des manifs :

- Un nombre minimum de participants : l'action est annulée ou modifiée par un plan B de moindre intensité si le nombre de participants minimum nécessaire n'est pas atteint.
- Des stratégies de fuite : à quel moment partir, comment le communiquer aux autres, où se séparer, comment éviter d'être suivis, comment vérifier que chacun·e est rentré à la maison sans problème ?
- Des points de rassemblement : se regrouper avant de se rendre vers le site d'une action.
- Des tactiques de rue appropriées : se positionner en deux lignes avec des rôles complémentaires par exemple.

- Des pratiques de communication claires : comment communiquer dans la rue, est-ce que vous amènerez vos téléphones[2], quels noms utiliser entre vous ?
- Des moments de débriefing : comment vérifier entre vous après l'action que tous sont en sécurité, se rassembler plus tard pour faire un retour sur l'action ou offrir du soutien.

Différents groupes vivent différentes **expériences de culture de la sécurité** et je ne tenterai pas de parler de tout. J'aimerais plutôt en partager quelques-unes dont j'ai fait l'expérience avec les gens qui m'entourent et qui nous ont réussi. Il s'agit de la vérification d'identité, du *vouching*, des cercles de confiance, des structures organisationnelles flexibles et du fait d'aborder les mauvaises dynamiques de façon proactive.

La **vérification d'identité** sert à établir qu'une personne est bien qui elle prétend être[3]. Lors de la mobilisation contre l'oléoduc décrite plus haut, au moment où on a voulu passer à des actions directes plus intenses, on a eu besoin d'approfondir la confiance au sein du groupe. Parce qu'on parlait régulièrement de risques, on a compris que les pratiques de sécurité utilisées pour les manifs, les petites occupations et les événements de sensibilisation n'étaient pas adaptées à nos nouveaux objectifs. Comme on s'inquiétait du risque d'infiltration, on a décidé de vérifier les identités des uns et des autres. Par exemple, je pouvais inviter une personne à prendre un café et, sans prévenir, montrer ma carte d'identité et peut-être une photo de famille ou une photo de classe. Je pouvais lui dire que je voulais qu'iel puisse avoir confiance que j'étais réellement celle que je prétendais être parce que je voulais qu'on puisse mener ensemble des actions plus risquées. On discutait ensuite de ce que cette personne pourrait me montrer. Parfois, il s'agissait d'un coup de fil à son travail ou à un membre de sa famille en haut-parleur. Je pouvais ainsi entendre la voix de la personne à

[2] *NdNTP :* Nous déconseillons d'apporter un téléphone lors d'une manifestation qui comporte des risques d'arrestation, sauf s'il s'agit d'un téléphone acheté pour l'occasion de manière anonyme, et équipé d'une carte SIM également achetée pour l'occasion pour manière anonyme.

[3] *NdNTP :* D'autres techniques que la vérification d'identité peuvent être utilisées pour vérifier qu'une personne est bien qui elle prétend être. Pour plus d'informations, voir notre Threat Library[4].

[4] https://notrace.how/threat-library/mitigations/background-checks.html